UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,835	05/10/2001	William Ray Cooley	P0367	6454

23735 7590 07/17/2006

DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/853,835	**Applicant(s)** COOLEY ET AL.	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 May 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,17-27,29-37 and 39-42* is/are pending in the application.

4a) Of the above claim(s) *14-16,28 and 38* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,17-27,29-37 and 39-42* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1—13, 17-27, 29-37, and 39-42 are pending.

Claims 14-16, 28, and 38 have been cancelled.

2. This is a Non-Final rejection.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/3/2006 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-13, 17-25 and 39-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan, et al. (US 6,801,999).

As per claim 1:

Venkatesan, et al. discloses a method of regulating access to a website by a user terminal via the Internet, the user terminal reading a physical object including embedded steganographic indicia, said method comprising:

at the user terminal, extracting identifying data from the steganographic indicia, and providing the identifying data to a remotely located central computer; **[col.29, lines 46-50 and col.31, lines 62-65; As indicated in applicants specification steganographic is in the form of digital watermarking technology. Hence, Venkatesan teaches digital watermark]**

at the central computer:

identifying a pointer associated with the identifying data; **[col.5, lines 26-27 and col.13, lines 45-51 and 56-67]** generating at least one component of response information; storing the response information; and **[col.28, lines 1-6 and col.29, lines 49-51]**

providing the pointer and response information to the user terminal; **[col.14, lines 25-36 and col.29, lines 52-56]**

at the user terminal, communicating with the website the pointer **[col.22, lines 6-20]** via and providing the response information to the website; **[col.27, lines 55-58 and col.30, line 11-17]**

at the website, communicating verification information to the central computer; and **[col.13, lines 37-38]**

at the central computer, verifying authority to access the website based at least in part on a comparison of the verification information **[col.28, lines 17-21]** and the stored response information. **[col.29, lines 1-8]**

Venkatesan did not specifically explain the pointer comprising information to access a website. However, it is obvious that the pointer includes information such as keys, header, or license that depicts permission and rights to access to the watermarked object pointing to a location such as a website (col.23, lines 9-67). The claimed identifying data is broad, thus the identifying data that is associated with the pointer can be keys or information within a header (col.23, lines 52-67). Venkatesan discloses the starting location (pointer) is determined by a corresponding different one of the keys (identifying data) that are used for all objects that are to be protected. The claimed pointer is Venkatesan's starting location points to a location in a protected object and also in terms of a relative byte address (col.5, lines 26-27 and col.13, lines 45-51 and 56-67) or the appropriate hyperlink for the client PC to execute on (col.14, lines 25-36). Venkatesan discusses the claimed pointer comprises information to access a website (col.15, lines 47-60) where the information is in the header such that when a user attempts to access and use encrypted object files, the ES reads the header from this file and passes the header to the license verifier (col.23, lines 52-67 and col.29, lines 52-56). Further, Venkatesan's invention is suited for use with downloading Internet accessible software objects from an Internet web site maintained by a content provider (i.e. publisher) to a client PC (col.10, lines 34-39). Therefore, it would have been obvious for a person of ordinary skills in the art that Venkatesan discloses a pointer comprising information to access the website because the information points to the location of the watermarked object and is necessary to have the information to execute on an appropriate hyperlink for that object in order to download form a web site (ol.10, lines 34-39 and col.14, lines 25-36).

As per claim 2: See col.13, line 30 and col.14, lines 34-35; discussing the identifying data comprises an object identifier.

As per claim 3: See col.14, lines 26-27 and 29, lines 11-13; discussing the pointer comprises at least one of a URL, IP address and web address.

As per claim 4: See col.27, lines 10-14; discussing at least one component comprises a random number.

As per claim 5: See col.25, lines 18-22; discussing generating at least a second component, the second component comprising a time stamp.

As per claim 6: See col.25, lines 18-22 and col.27, lines 10-14; discussing the response information comprises at least the random number and the time stamp.

As per claim 7: See col.14, lines 34-35 and col.25, lines 18-22 and col.27, lines 10-14; discussing the verification information comprises at least the random number, the time stamp and a valid identifier.

As per claim 8: See col.14, lines 6-8 and col.23, line 9-12; discussing verifying authority comprises indexing the stored response information via the communicated random number and determining whether the stored response information matches the valid identifier and whether the verification information is received within a predetermined time period.

As per claim 9: See col.11, lines 33-46; discussing when the stored response information matches the valid identifier within the predetermined time period, method further comprising authorizing user terminal access to the website.

As per claim 10: See col.17, lines 50-64; discussing when the stored response information does not match the valid identifier or the verification information is not received within the predetermined time period, comprises signaling a lack of authority for the user terminal to access the website.

As per claim 11: See col.17, lines 50-64 and col.27, lines 11-16; discusses verifying authority comprises indexing the stored response information via the valid identifier and determining whether the stored random number matches the communicated random number, and whether the verification information is received within a predetermined time period.

As per claim 12: See col.14, line 15 and col.18, line 49; discusses encrypting at least one component of the of the response information.

As per claim 13: See col.17, lines 41-42 and 27, lines 10-13; discussing the document identifier is randomly generated.

As per claims 14-16: **Cancelled**

As per claim 17:

Venkatesan teaches a method of authenticating permission to access a system comprising:

receiving a request to enter the system, the request including at least a verification key protected **[col.6, lines 2-4]**, the request being associated with at least a steganographically marked object; **[col.27, lines 58-59 and col.29, lines 14-15 and 46-50; As indicated in applicants specification steganographic is in the form of digital watermarking technology]**

querying a data structure to determine whether the verification key is authorized; **[col.7, lines 34-38 and col.11, lines 40-46]**

allowing access to the system based on the response to the query; and **[col.5, lines 24-56 and col.24, lines 42-46; Venkatesan discusses querying the database for comparing the value of the watermark in the license to the value of the actual corresponding watermark to determine if there is a match to permit access]**

verification key comprises a first random number **[col.14, lines 3-5 and col.27, lines 5-14]**, and the data structure comprises at least one data record including a second random number and a first identifier. **[col.24, line 59-col.25, line 10]**

Venkatesan does teach the verification key in the form of watermark key, that is generated by the watermark authority (WA) for objects that are to be protected (col.6, lines 2-4). There are also other information (i.e. header, license) that permits access to the watermarked object (col.19, lines 3-6) but did not specifically discuss the allowing access to the system. Venkatesan discusses watermarking the objects and a provides a resulting watermarked version of that object is for the publisher where the publisher distributes resulting encrypted, fingerprinted and watermarked copies of the object to requesting users (col.6, lines 8-21). After a user has downloaded a watermarked object and in order to use that object the user transacts to the Internet with publisher's web server and pays for a specific licensing fee to the publisher that contains access rights to the client. Further, Venkatesan's invention is suited for use with downloading Internet accessible software objects form an Internet web site maintained by a content provider (i.e. publisher) to a client PC (col.10, lines 34-39). Therefore, it would have been obvious for a person of ordinary skills in the art for having verification information such as keys of Venkatesan to allow access to the publisher's system to download the objects.

As per claim 18: See col.17, lines 32-64; discussing the verification key further comprises a first time stamp and the data record further includes a second time stamp.

As per claim 19: See col.24, line 59-col.25, line 10 and col.27, lines 10-14; discussing indexes the data record via the first random number, the first and second random numbers (col.14, lines 3-5 and col.27, lines 5-14) being equal, determines whether the first identifier matches the second identifier, and whether the first time stamp is within a predetermined time range based on the second time stamp, and signals to the system whether the first identifier matches the second identifier and whether the first time stamp is within the predetermined time range.

As per claim 20: See col.25, lines 7-8; discussing the first identifier comprises an identifier extracted from a digital watermark.

As per claim 21: See col.23, lines 10-25 and col.25, lines 18-22 and col.27, lines 10-14; discussing indexes the data record via the second identifier, the first identifier and second identifier being equal, determines whether the first random number matches the second random number, and signals to the system whether the first random number matches the second random number and whether the verification information is received within a predetermined time.

As per claim 22:

Venkatesan discloses a system for exchanging data comprising:

a central server comprising at least one database **[col.28, lines 1-6 and col.29, lines 49-51]** including response information and pointer information **[col.27, lines 55-58 and col.29, lines 52-56]**, wherein when a user terminal communicates an extracted watermark identifier to said central server **[col.25, lines 5-11 and col.31, lines 62-65; As indicated in applicants specification**

steganographic is in the form of digital watermarking technology], said central server identifies a corresponding URL with the extracted watermark identifier **[col.15, lines 47-58 and 23, lines 46-51]**, and wherein said central server generates a number**[col.27, lines 5-15]**, and stores the number and extracted watermark identifier in the database as response information. **[col.31, lines 58-65]**

Venkatesan did not specifically explain the pointer comprising information to access a website. However, it is obvious that the pointer includes information such as keys, header, or license that depicts permission and rights to access to the watermarked object pointing to a location such as a website (col.23, lines 9-67). The claimed identifying data is broad, thus the identifying data that is associated with the pointer can be keys or information within a header (col.23, lines 52-67). Venkatesan discloses the starting location (pointer) is determined by a corresponding different one of the keys (identifying data) that are used for all objects that are to be protected. The claimed pointer is Venkatesan's starting location points to a location in a protected object and also in terms of a relative byte address (col.5, lines 26-27 and col.13, lines 45-51 and 56-67) or the appropriate hyperlink for the client PC to execute on (col.14, lines 25-36). Venkatesan discusses the claimed pointer comprises information to access a website (col.15, lines 47-60) where the information is in the header such that when a user attempts to access and use encrypted object files, the ES reads the header from this file and passes the header to the license verifier (col.23, lines 52-67 and col.29, lines 52-56). Further, Venkatesan's invention is suited for use with downloading Internet accessible software objects from an Internet web site maintained by a content provider (i.e. publisher) to a client PC (col.10, lines 34-39). Therefore, it would have been obvious for a person of ordinary skills in the art that Venkatesan discloses a pointer comprising information to access the website because the information points to the location of the watermarked object and is necessary to have the information to execute on an appropriate hyperlink for that object in order to download form a web site (ol.10, lines 34-39 and col.14, lines 25-36).

As per claim 23: See col.11, lines 39-45 and col.15, lines 51-52; discussing at least one database comprises a first database for storing pointers and a second database for storing response information.

As per claim 24: See col.25, lines 20-22; discussing server further generates a time stamp and stores the time stamp with the response information.

As per claim 25: See col.13, line 35 and col.25, lines 20-22; discussing the number comprises at least one of a random number, a pseudo-random number, and a predetermined number.

As per claim 39:

Venkatesan discloses a method of regulating access to a website by a user device over a network, the user device reading an object including hidden steganograhpic indicia, said method comprising:

receiving identifying data extracted from hidden steganograhpic indicia, wherein the identifying data was extracted by a remotely located user device and communicated via a network; **[col.29, lines 46-50 and col.31, lines 62-65; As**

indicated in applicants specification steganographic is in the form of digital watermarking technology]

identifying a pointer associated with the identifying data **[col.5, lines 26-27 and col.13, lines 45-51 and 56-67]**

providing at least one component of response information; storing the response information; **[col.28, lines 1-6 and col.29, lines 49-51]**

communicating the pointer and response information to the user device via the network **[col.22, lines 6-20]**, whereby the user device may access the website using at least the pointer and provide the response information to the website; **[col.27, lines 55-58 and col.30, line 11-17]**

receiving verification information **[col.6, lines 2-4]** from the website including at least a portion of the response information; **[col.28, lines 17-21]**

verifying authority to access the website based at least in part on a comparison of at least a portion of the verification information and at least a portion of the stored response information; and **[col.29, lines 1-8]**

providing an indication of authority to the website. **[col.28, lines 32-42]**

Venkatesan did not specifically explain the pointer comprising information to access a website. However, it is obvious that the pointer includes information such as keys, header, or license that depicts permission and rights to access to the watermarked object pointing to a location such as a website (col.23, lines 9-67). The claimed identifying data is broad, thus the identifying data that is associated with the pointer can be keys or information within a header (col.23, lines 52-67). Venkatesan discloses the starting location (pointer) is determined by a corresponding different one of the keys (identifying data) that are used for all objects that are to be protected. The claimed pointer is Venkatesan's starting location points to a location in a protected object and also in terms of a relative byte address (col.5, lines 26-27 and col.13, lines 45-51 and 56-67) or the appropriate hyperlink for the client PC to execute on (col.14, lines 25-36). Venkatesan discusses the claimed pointer comprises information to access a website (col.15, lines 47-60) where the information is in the header such that when a user attempts to access and use encrypted object files, the ES reads the header from this file and passes the header to the license verifier (col.23, lines 52-67 and col.29, lines 52-56). Further, Venkatesan's invention is suited for use with downloading Internet accessible software objects from an Internet web site maintained by a content provider (i.e. publisher) to a client PC (col.10, lines 34-39). Therefore, it would have been obvious for a person of ordinary skills in the art that Venkatesan discloses a pointer comprising information to access the website because the information points to the location of the watermarked object and is necessary to have the information to execute on an appropriate hyperlink for that object in order to download form a web site (ol.10, lines 34-39 and col.14, lines 25-36).

As per claim 40: See col.32, lines 38-39; discussing the indication inhibits access to the website.

As per claim 41: See col.6, lines 62-65; discussing the indication allows access to the website.

As per claim 42: See col.5, line 20; discussing the user device comprises a handheld device.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 26-27 and 29-37 are rejected under 35 U.S.C. 102(e) as being anticipate by Moskowitz, et al. (US 5,822,432).

As per claim 26:

Moskowitz teaches a method of operating a computer server, the computer server to communicate with at least one user terminal, said method comprising:

receiving an object identifier from the user terminal, wherein the object identifier is steganographically embedded in the object; **[col.9, lines 1-16 and 44-45; As indicated in applicants specification steganographic is in the form of digital watermarking technology where data are hidden (by embedding) in some other object]** identifying a pointer associated with the document identifier **[col.6, lines 24-25]** wherein the pointer comprises at least one of a URL, IP address and web address; **[col.9, lines 29-39]**

generating at least one component of response information; **[col.9, lines 17-24]**

storing the response information; and **[col.5, lines 35-39 and col.6, lines 25-40]**

providing the pointer and response information to the user terminal. **[col.9, lines 33-38]**

As per claim 27: See col.3, lines 23-25; discussing the object identifier is steganographically embedded in the form of a digital watermark.

As per claim 28: **Cancelled**

As per claim 29: See col.6, lines 17-18; discussing the at least one component comprises a random number.

As per claim 30: See col.9, line 41; discussing the response information further comprises a time stamp.

As per claim 31: See col.6, lines 17-18 and col.9, line 41; discussing the response information comprises at least a random number and a time stamp.

As per claim 32: See col.6, lines 17-20 and col.9, lines 40-51; discussing verifying data, wherein said verifying data comprises indexing the stored response information via a second random number, and determining whether the stored document identifier matches a valid identifier.

As per claim 33: See col.9, lines 17-21 and 40-51; discussing when the stored document identifier matches the valid identifier, said method further comprises authorizing user terminal access.

As per claim 34: See col.3, lines 43-58 and col.9, lines 25-26; discussing when the stored document identifier does not match a valid identifier, said method further comprises signaling a lack of authority for the user terminal.

As per claim 35: See col.6, lines 17-20 and col.9, lines 40-51; discussing verifying data comprises indexing the stored response information via a valid identifier and determining whether the stored random number matches a second random number.

As per claim 36: See col.6, line 16-20; discussing encrypting at least one component of the response information.

As per claim 37: See col.3, line24-26; discussing the document identifier is randomly generated.

As per claim 38: **Cancelled**

Response to Arguments

6. Applicant's arguments filed October 31, 2005 have been fully considered but they are not persuasive.

Venkatesan teach the central server in the form of the Watermark Authority (WA) that is a third party wherein the WA is remotely located from the client PC and the Publisher (see FIG.15 and 16). Applicant's web site is disclosed in Venkatesan as the publisher that maintains a web server providing a web site (col.14, lines 26-28). Thus, the web site is referred hereinafter as the publisher. Hence, the WA accesses the publisher based at least in part on a comparison of the verification information (col.28, lines 17-21) and the stored response information (col.29, lines 1-8). Identifying data is broad, thus identifying data associated to a pointer can be keys. The claimed pointer is Venkatesan's starting location points to a location in a protected object and also in terms of a relative byte address. The starting location (pointer) is determined by a corresponding different one of the keys (identifying data) that are used for all objects that are to be protected (col.5, lines 26-27 and col.13, lines 45-51 and 56-67). Venkatesan teaches the verification key in the form of watermark key, that is generated by the watermark authority (WA) for objects that are to be protected (col.6, lines 2-4). Venkatesan further discloses the corresponding watermark specified by the watermark key stored within the key manager and the corresponding watermark exists in decrypted object where the key manager provides the watermark key for client PC. The watermark key serves as a pointer in time, space, or frequency as appropriate to the corresponding watermark embedded in the object where examines the object to locate the corresponding watermark therein and inform the license verifier. Further, the watermark is located and extracts an actual value of the watermark embedded in object M and provides this value to the verifier where the verifier compares the VID value contained in header and the PID value specified in the license to actual VID and PID values extracted from the watermark detected in the object to determine if identical matches exists (col.24, line 59-col.25, line 10).

As per claim 14, recites requesting to enter the system, "the request including at least a verification key, the request being associated with at least a steganographically marked object" where the limitation merely receiving a request to enter a system which broadly leaves this limitation open to receiving at any system. Thus, receiving a request including a verification key to enter a system can broadly be given in light to either the publisher's system or the WA system of Venkatesan. Venkatesan discusses seeking to access the server (col.11, lines 26-30) to download the locked object wherein a request (col.29, lines 14-15 and col.33, lines 42-450) includes a file that contains a key for verification in order to access the object (col.14, lines 27-48). Further, Venkatesan discusses in the case of a media card, WA provides one key to a card manufacturer where during manufacturing of the card, the key is embedded in encrypted form where the key is detects the presence of the corresponding one of the n watermarks in the protected objects (col.15, lines 15-18).

As per claim 22, Venkatesan discusses the watermark having a value (identifier) that is extracted and sent from the user to compare to a value of the corresponding watermark stored in the object wherein the secret specifies a location (col.11, lines 40-46) or the address in terms of spatial domain key (col.13, lines 57-63) and is stored in the database as response information (col.33, lines 53-55). The identifier values can be the publisher ID (VID) and the product ID (PID) where these values from the watermark are extracted to determine a corresponding value (col.25, lines 5-11).

Claim 39, the identifying data is broad, thus identifying data associated to a pointer can be keys. The claimed pointer is Venkatesan's starting location points to a location in a protected object and also in terms of a relative byte address. Venkatesan discloses the starting location (pointer) is determined by a corresponding different one of the keys (identifying data) that are used for all objects that are to be protected (col.5, lines 26-27 and col.13, lines 45-51 and 56-67). Venkatesan discusses the claimed pointer comprises information to access a website (col.15, lines 47-60) where the information is in the header such that when a user attempts to access and use encrypted object files, the ES reads the header from this file and passes the header to the license verifier (col.23, lines 52-67).

According to the specification, digital watermarking technology is a form of steganography, which digital data are hidden in some other objects. Digital watermarks inherently embed data for verification/authentication purposes, which is hiding the data. Therefore, Moskowitz teaches embedded data exists in the digital watermark, is applicant's steganographic indicia.

Claim 26 broadly recite, "identifying a pointer associated with the object identifier, wherein the pointer comprises at least one of a URL, IP, and web address" where this limitation merely points to a location (i.e. URL, IP, address) of the object. The claim fails to limit pointing to a particular type of object and only recites an object identifier. The identifier for an object can be given its broadest and reasonable interpretation is data that identifies the object. Therefore, identifier of an object can be the watermark random generated key (col.1, lines 39-42) or the digital notary that contains a unique identification number (col.9, lines 40-49). Moskowitz discusses watermarks contain information pertaining to geographical or electronic distribution restrictions or this information points to the URLs of online sites of the similar content. Moskowitz does teach identifying a pointer associated with the document identifier (col.6, lines 24-25) wherein the pointer comprises at least one of a URL, IP address and web address (col.9, lines 29-39).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HOSUK SONG
PRIMARY EXAMINER

LHa